Barnardo's

Submission to the call for evidence on the Age Appropriate Design Code – Information Commissioner

September 2018

[redacted]

About Barnardo's

1. Barnardo's is the UK largest children's charity supporting over 301,100 children, young people, parents and carers through over 1,000 services across the UK. Our services provide counselling for children who have been exploited, support for children in and leaving care and specialist mental health services. Barnardo's purpose is to transform the lives of the most vulnerable children and young people. We work to build stronger families, safer childhoods and positive futures for children and their parents and carers through our services, campaigns and research.

2. Barnardo's would be happy to assist the ICO in gathering the views of children, parents, carers, and practitioners on age-appropriate design and the proposed Code. Please get in touch using the contact details above.

Overview

3. The response below sets out Barnardo's assessment of the challenges that face children in their use of technology and the internet, as well as recommendations for how the Code should seek to address them.

4. We are keen for the ICO to make clear that the Code's fundamental purpose is to enable children to be safe and confident in their use of online services, aware of risk but not unduly concerned or constrained by it. The Code can achieve this by ensuring that internet services (and internet-enabled technology) are *safe by design* and properly consider the best interests of child users from the outset, in all that they do. Principally, this means:

    - **Privacy by default** – high privacy should be embedded in each standard of the Code, and therefore in every online service or device used by children. Technology companies, not parents, carers, or children themselves, must be held ultimately responsible for protecting the privacy of children and young people online.
    - **Transparency by default** - nothing should prevent children and young people, or their parents and carers, from being informed in their use of technology and the internet. Transparency, which includes communicating

clearly and honestly, means online service providers being open not just about their policies and settings, but also about the intent behind them.
- **Co-design** – safety by design can only be achieved with a thorough understanding of how children and young people use online services. Just as the Code must be developed in close consultation with children, parents, and carers, including the most vulnerable children, so should internet services and devices themselves.

5. The evidence set out below has been gathered from both external sources and from Barnardo's own work supporting children and young people. This response largely draws on our particular areas of concern and experience, but for further evidence on the full range of design areas to be covered by the Code, please see the response of 5rights, and CHIS to which Barnardo's is a signatory.

Summary of recommendations

- As above, high **privacy by default** and **transparency by default** standards should be required for all services and devices used by children.
- Online services' **terms and conditions should be simplified and standardised**, making them easier for children to understand.
- **Geolocation should be off by default** on all services and devices where it is not a core part of the service.
- The automatic or semi-automatic **profiling of children should be prohibited in law**, and only allowed when the ICO deems it to be in the best interests of the child. Where children are profiled, they should be able to understand how their profiles have been developed and have recourse to challenge them.
- **Child users should have more control over changing/disabling so-called persuasive design features**, allowing them to better manage their online use and screen time.
- **Universal, standardised reporting and resolution procedures** should be enforced, including time limits for responding and clear appeals processes, so that children are better able to report concerning or harmful content.
- **Children's right to erasure and rectification should be expedited** and the best interests of children should always be prioritised in resolution processes.
- **Guidance for children of different ages/stages of development on data rights and privacy** should be published alongside the Code, with the needs of children with learning difficulties properly taken into account. Online services should be required to signpost children to independent sources of advice and support.
- Companies should be required to report on how they have considered the impact on children's rights/wellbeing in their design, as well as **demonstrate how they have included children in the design process.**
- The ICO should consider the impact of including **dedicated standards on age-verification and facial/voice recognition** in the Code.
- The Code should require technology companies to **have regard to the particular needs of different groups of children**, including disabled children, children with special educational needs, and vulnerable groups of children such

as those who are in care. A one-size-fits all approach to design will lead to many children being failed.

Development needs of children at different ages (Q1-2)

1. Broadly-speaking, Barnardo's supports the proposed age ranges as being appropriate proxies for children's development during infancy, childhood, and adolescence.

2. It is important to note, however, that while development may broadly correspond to age for the majority of children and young people, this is not always the case, particularly for the most vulnerable groups of children. Our growing understanding of brain development shows us that those who have experienced early trauma and ACEs (Adverse Childhood Experiences) can develop at a different pace to their peers,[1] meaning that chronological triggers are not, in and of themselves, a safeguard for all children and young people. The same applies to children with learning disabilities, of course.

3. This underlines for us the importance of requiring online services to be absolutely clear and transparent in the way that children's data is collected or shared, dependent on the different privacy settings available. Children, or those involved in their care, are often in the best position to determine their developmental stage, irrespective of their age, which means that they must be able to inform themselves about the specific protections in place as children grow up. Children, and those who support hem, must be able to easily understand what happens to their information when they sign up to an online service, and not rely solely on the age guidelines to determine whether or not to accept these terms and conditions.

4. Moreover, we do not believe that the Code should simply accept 13 as the age at which children are considered either capable of giving their consent to have their data processed or competent enough more generally so as to require less stringent protections. While the GDPR allows member states to use this age (as a minimum), and the UK has chosen to, we do not see any justification for this. Indeed, the UK Government itself appears not to accept that children are Gillick competent at 13 either, given its decision this year to extend the right of withdrawal from relationships and sex education (RSE) to children only at age 15.[2] We would also note that children under the age of 16 cannot legally consent

---

[1] Perry, B (2004) *Maltreatment and the Developing Child*, The Centre for Children & Families in the Justice System, https://childtrauma.org/wp-content/uploads/2013/11/McCainLecture_Perry.pdf

[2] Written Ministerial Statement, Relationships and Sex Education, Rt Hon Damian Hinds MP, July 2018: https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2018-07-19/HCWS892/

to sexual communications from adults,[3] but are explicitly exposed to this risk, often with no protections whatsoever, through a number of online services.[4]

5. We commend the ICO for making efforts to establish the evidence base for the relative competence of children online, and look forward to seeing this evidence reflected in the standards the Code enforces for different ages.

6. Finally, we would warn against the Code adopting an approach that broadly-speaking sees standards relaxed as children get older. While children's competence online may increase as they get older, so too does the level of risk they are subject to, whether by virtue of increased use, different types of use, increased freedom, or other changes and pressures experienced in the offline world. Children may merit different kinds of protection under the Code based on their age, but in our view they do not merit different levels of protection. For this reason, as well as those outlined above, we believe the ICO should also consider how it might require online services to allow users to maintain all their child-user settings even after they've reached the age of 18.

The United Nations Convention on the Rights of the Child (Q3)

7. The principle enshrined in Article 3 of the UNCRC – that 'the best interests of the child shall be a primary consideration' – is central to Code and its design standards. As such, online service providers must be in no doubt that children's right to privacy (Article 16), or protection from abuse and exploitation (Articles 19 and 34), or protection from harmful material (17e), takes priority over any incentive they might have to share, sell, or simply collect children's data.

8. The Code should also require online service providers to have regard to Article 12, which dictates that the views of children are taken into account in all decisions affecting them. Children and young people ought to be informed in their use of the internet, but this isn't possible if, for instance, terms and conditions are impenetrable, profiling is unintelligible, or reporting and resolution processes are inconsistent and opaque. In addition to demanding privacy-by-default, therefore, the Code must also demand transparency-by-default. If there is no good reason for service providers to hide their processes, policies, or intentions from children, they should not be allowed to.

Aspects of design – challenges and recommendations (Q4-5D)

---

[3] See section 15A, Sexual Offences Act (2003): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/604931/circular-commencement-s67-serious-crime-act-2015.pdf

[4] See Net Aware report 2017: https://learning.nspcc.org.uk/research-resources/2017/net-aware-report-2017-freedom-to-express-myself-safely/

Default privacy settings

Challenges

9. Setting strict, enforceable rules around default settings in the Code is vital, because in practice defaults stay in place for the vast majority of users. Only 18% of child users (12-15 years old) change their settings on social media.[5] Different privacy settings are also not readily understood – for instance, UKCCIS found that 26% of child social media users did not know the difference between a public and a private profile.[6]

10. This problem was highlighted by interviews conducted by Barnardo's with some of the young people supported through its services. One of those interviewed, Debbie, aged 15, started using Facebook at age 12 and would be added to strangers' lists of friends:

    a. 'they added me and they were talking to me at first and then they asked for pictures. Some I said no to, some I didn't really want to but I thought – well if they like me then I felt I had to.'[7]

11. Awareness of their privacy online varies from child to child, and many children are not aware that the settings they have in place often allow people to contact them freely on social media. Unless default settings deliver a high degree of privacy, children like Debbie will continue to be vulnerable.

Recommendations

12. The Code should enforce a high privacy by default standard on all devices and services that are accessed by children. Clear, age-appropriate explanations of different privacy settings and their impact should be presented to child users at regular intervals, as well as every time an account is created or settings are changed.

Terms and conditions and privacy notices

Challenges

13. In focus groups carried out by Barnardo's this year, young people stated that social media and internet companies needed to inform users more clearly about

---

[5] Livingstone S et al (2017) Children's Online Activities, Risks and Safety: a Literature Review by the UKCCIS Evidence Group, London School of Economics and Political Science: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf

[6] Ibid.

[7] Palmer, T (2015) Digital Dangers: the impact of technology on the sexual abuse and exploitation of children and young people, Barnardo's http://www.barnardos.org.uk/onlineshop/pdf/digital_dangers_report.pdf

privacy and safety features, as well as be more accountable for young people's safety.[8]

14. Due to both their length and complexity, the reality of most online service terms and conditions is that most users do not – or, practically, cannot – read the terms and conditions of every site they visit or app they use.[9] Even if they could, the ability to give meaningful consent is dependent on the evolving capacity of individual children at different ages, taking into account any special education needs or disabilities that they may have.

Moreover, the inflexibility and non-negotiability of terms and conditions limits the extent to which consent can be considered meaningful, and children are unlikely to see the point in reading something they effectively have to accept anyway.

Recommendations

15. Terms and conditions should be simplified and standardised, and presented in clear, age-appropriate language. The Children's Commissioner for England has already demonstrated that this is possible, working with lawyers to produce simplified T&Cs in 2017 for websites and apps popular among children, including Facebook, Instagram, Snapchat, Youtube, and Whatsapp. The new T&Cs are designed to be accessible and child-friendly, allowing children and young people to better understand their rights – tech companies should be required to follow their lead.[10] They should also be communicated at regular intervals, not simply at inception.

16. As part of the Code, the ICO should publish guidelines to children's consent, thereby placing it on a statutory footing. If it is demonstrated that terms and conditions are consistently difficult for children to understand, the online service should be required rewrite them and seek fresh consent from all its users.

Geolocation technology

Challenges

17. The pervasive use of geolocation features by ISS, particularly social media sites presents a number of risks to children and young people. A 2016 survey of Barnardo's sexual exploitation services in the UK revealed that of the children supported by those services who were groomed online, two-thirds (61%)

---

[8] Focus groups carried out by Barnardo's as part of its submission to the Government's consultation on 'Transforming Children and Young People's Mental Health Provision' (February 2018)

[9] Research by the BBC in 2018 found that the reading age of some popular apps' terms and conditions were at university level, and that reading the T&Cs of all 15 popular sites surveyed would take almost nine hours: https://www.bbc.co.uk/news/business-44599968

[10] https://www.childrenscommissioner.gov.uk/publication/simplified-social-media-terms-and-conditions-for-facebook-instagram-snapchat-youtube-and-whatsapp/

subsequently met the perpetrator and were sexually exploited.[11] There is clearly a risk that geolocation technology may be used to assist such online-facilitated sexual exploitation. Further, in a recent study of female survivors of intimate partner violence, for instance, 56% reported that their partners had used technology to check up on their whereabouts and 17% reported that their location had been tracked using geolocation technology.[12]

18. These risks are exacerbated by the fact that location-sharing is often a condition of service (e.g. Snapchat), or are active even when apps are not in use (e.g. Instagram). This is despite these features not being necessary or even particularly beneficial to the user experience in many cases. As a result, highly sensitive information about children can be gleaned easily from geolocation data, including where they live, go to school, or hang out.

Recommendations

19. A child's location should be classed as sensitive data by the Code. This would, in effect, add a child's location as a 'special category of personal data' alongside those other categories that cannot be processed without consent under Article 9(1) of the GDPR.

20. Short of this, and more generally where geolocation features are not critical to a service, they should be off by default for child users. Any online service that uses geolocation features, whether a core part of their service or not, should be required to notify their child users at regular intervals that geolocation features are on, as well as issue a simple and standardised disclaimer informing children about the practical implications of having these features enabled.

21. The principle of data-minimisation should also be central to the standard on geolocation. For instance, if the service does not require geolocation data to be collected or stored when the service is not in use, either because a child has logged-out or simply navigated away, then it shouldn't be.

Automated and semi-automated profiling

Challenges

22. Profiling is a two-way street. Whilst it can be used to improve children's experience based on existing traits or tastes, it can equally have the effect of shaping or influencing children's identity and behaviour in unwanted or harmful ways. For instance, while most social media sites seek to moderate/filter out pro-eating disorder and harmful body image content, recent research has found

---

[11] Barnardo's online grooming survey 2016: http://www.barnardos.org.uk/barnardos-online-grooming-survey-2016.pdf

[12] Woodlock D. (2016) The abuse of technology in domestic violence and stalking. Violence Against Women: http://journals.sagepub.com/doi/full/10.1177/1077801216646277

that some sites are actually suggesting this kind of content to their users through their profiling algorithms.[13]

23. Irrespective of the risks associated with profiling, however, children and young people have little understanding about how profiling works and are largely unaware of the specific profile that they have accrued. In fact, a report published by the ICO last year found that only 23% of online services provide information about how a child could contest an automated/semi-automated decision made on the basis of their profile.[14]

Recommendations

24. Barnardo's recommends that the profiling of children is prohibited in law, unless the Information Commissioner determines that it is in the best interests of the child. If an online service wish to profile children, it should be required to produce an impact assessment and apply to the Commissioner for an exemption.

25. Where the profiling of children is permitted, online services should take steps to keep child users informed about the nature of their profile, its implications, and how it is developed. The Code should also require online services to have processes in place for child users to question and/or seek amendments to their profile if necessary.

The strategies used to encourage extended user engagement

Challenges

26. Barnardo's is keen to emphasise that while technology and the online world comes with risk, it also provides considerable benefit and opportunity for children and young people. For example, an online poll conducted for Barnardo's showed that access to the internet helps three-quarters (75%) of today's young teenagers to do their schoolwork, compared with 44% of 25-34 year olds when they were the same age. [15]

27. However, research shows a clear link between excessive use of social media and mental health problems. Recent analysis conducted by Barnardo's and The Children's Society found that children with heavy social media use 'were

---

[13] Gerrard, Ysabel (2018) Beyond the hashtag: Circumventing content moderation on social media, New Media and Society
http://journals.sagepub.com/doi/abs/10.1177/1461444818776611

[14] GPEN SWEEP 2017: User Controls over personal information. Global Privacy Enforcement Network, UK Information Commissioners Officer:
https://www.privacyenforcement.net/sites/default/files/2017%20GPEN%20Sweep%20-%20International%20Report.pdf

[15] Survey reveals transformation of childhoods in a digital world, 2018:
https://www.barnardos.org.uk/news/Survey-reveals-transformation-of-childhoods-in-a-digital-world/press_releases.htm?ref=126384

significantly more likely to have subsequent mental health problems',[16] and 38% of young people report that social media has a negative impact on how they feel about themselves. The situation is worse for girls, 46% of whom state that social media has a negative impact on their self-esteem. [17]

28. Excessive use can impact on children's physical or other activity too. An online poll[18] conducted for Barnardo's showed that:

    a. The number of young teenagers who play outside, read books or get enough sleep has dropped sharply in comparison to teenagers from previous decades[19]
    b. The study found half (54%) of those aged 13-15 read books. By contrast, 79% of adults aged over 18 said they did so when they were young teenagers.
    c. Just half (50%) of today's young teenagers believe they get sufficient sleep against two-thirds (66%) of adults who said they did so when they were aged 13-15.

29. Despite these well-documented problems, self-regulation by the technology industry has been inadequate to date. Some online services have (ostensibly) started to tackle excessive use by providing time management controls. In 2018 Google added a 'digital wellbeing' banner to its Android P operating system, showing users how many times they've unlocked their phone, and time spent on apps and websites. Instagram has also prototyped a 'usage insights' feature that is expected to allow users to see the time they've spent on the app and set their own time limits. While these developments are to be welcomed, they do not represent a reduction in the use of persuasive design features and their effectiveness in mitigating compulsive or excessive use may therefore be limited.

Recommendations

30. The Code should require online services to be more transparent in their use of persuasive design features and give child users more freedom to change or disable them if they wish. For instance, the majority of apps that use push notifications simply give users the choice between having them on or off, with no control over how frequently they receive notifications, what time, or what

---

[16] Pople L. (2018) Factors affecting children's mental health over time, Barnardo's and The Children's Society: https://www.childrenssociety.org.uk/what-we-do/resources-and-publications/factors-affecting-childrens-mental-health-over-time

[17] Safety Net: Cyberbullying's impact on young people's mental health, Young Minds & The Children's Society, 2018: https://youngminds.org.uk/media/2189/pcr144b_social_media_cyberbullying_inquiry_full_report.pdf

[18] Barnardo's survey reveals transformation of childhoods in a digital world, 2017: https://www.barnardos.org.uk/news/Survey-reveals-transformation-of-childhoods-in-a-digital-world/press_releases.htm?ref=126384

[19] Ibid.

specifically they want or don't want to receive notifications about. This prevents children from managing their use in the way that they want to.

31. In developing the standard on strategies used to extend user engagement, the ICO should consult with children and young people on the design features that they believe present the most risk in terms of excessive use. Standards should reflect these concerns and the ICO should put procedures in place to regularly consult with children, and if necessary update the Code, as new features appear.

User reporting and resolution processes and systems

Challenges

32. Parents and carers often lack the skills to help their children to report things online, and children may be reluctant to ask for help depending on the nature of the content they are reporting. Barnardo's practitioners interviewed as part of research carried out in 2016 reported that the young people abused online with whom they had worked had not personally disclosed what had happened to them, with just one exception. One project worker said:

> 'Young people are silenced…they will never tell anybody – it's always about discovery. It is fear that surrounds disclosure regarding online abuse… and the largest facet of that fear is the fact that if they tell anyone there is every chance that the images they have sent and the language they have used may be seen and read. The anticipated embarrassment and the feelings of shame form the barrier to any disclosure.'[20]

33. The fact that reporting and resolution processes can be complicated, slow, and inconsistent further deters children from reporting, even if they would otherwise be minded too. And, as the above case study illustrates, children are unlikely to ask for help in resolving an issue online if it means disclosing the abuse in the first place.

Recommendations

34. Given that children and young people are often reluctant to disclose concerns they have online, reporting processes must be quick and easy. We would recommend the imposition of universal reporting standards, including similar or standardised reporting procedures, time limits for responding, and clear, standardised appeals processes.

35. To foster openness to user reporting, and to make online services accountable for their resolution processes, we also believe that the Code should include a

---

[20] Palmer, T (2016) Digital Dangers: the impact of technology on the sexual abuse and exploitation of children and young people, Barnardo's, Barkingside: http://www.barnardos.org.uk/onlineshop/pdf/digital_dangers_report.pdf

duty on all online services to produce annual transparency reports, detailing the number of reports, the kind of content that is reported, and their take-down/removal rates for different types of content. The ICO should review these reports and be able to request changes to online service policies/procedures in light of the findings.

The ability to understand and activate a child's right to erasure, rectification and restriction

Challenges

36. Children are increasingly accessing the internet at young ages and are generally not taught about their data rights.[21] It is little wonder, therefore, that more than one in four children and young people worldwide have regretted posting something online by age 16.[22] The same research found that 32% of children and young people have had to ask someone to remove content about them posted online. Given this, children or adults acting on behalf of children, must be able to activate their rights to erasure, rectification, and restriction easily and quickly.

37. The speed with which content is shared online or relationships can be developed means that an emphasis must also be placed on children being able to activate their rights quickly. Barnardo's research from 2015 revealed the case of one 10 year old girl – within two hours of engaging the child online, the perpetrator got her to send explicit images.

Recommendations

38. Responses to children's requests for erasure, rectification, and restriction should be expedited and protecting their privacy should be prioritised over defending free speech. This means that the process for managing children's rights to erasure, rectification, and restriction must be differentiated from processes for adults.

39. Child users should be regularly signposted towards information about how to activate their rights online, and as far as possible processes for erasure, rectification, and restriction should be standardised across services.

The ability to access advice from independent, specialist advocates on all data rights

---

[21] Children and Parents media use attitudes 2017, Ofcom: https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

[22] GPEN SWEEP 2017: User Controls over personal information. Global Privacy Enforcement Network, UK Information Commissioners Officer: https://www.privacyenforcement.net/sites/default/files/2017%20GPEN%20Sweep%20-%20International%20Report.pdf

Challenges

40. Parents, carers, and other trusted adults often lack the knowledge to provide children with advice about their online rights and safety. Indeed, a 2017 report published by Barnardo's in Scotland revealed that 'professionals noted that the speed of progress in technology made it difficult to keep up to date with how young people were using new media'.[23] As we have noted elsewhere, children may also be reluctant to share any concerns they have or problems they encounter online.

Case study

'It didn't cross my mind to ask her about what might be happening for her online. But it also didn't cross the minds of the GP or the school. It was 3 months from the point that I raised my concerns with the professionals about my daughter that I discovered through over hearing a conversation she was having, that she was planning to meet someone the next day right in the south of the country – 100 of miles from our home. I knew something was terribly wrong for her and that's why we went to the school and to the GP but neither we, nor they, asked the question. I didn't ask the question that needed asking because I didn't know about online grooming behaviours. Her teachers and GP didn't ask the question because they didn't think about what might be happening for Joanna online.' **Parent of Joanna, aged 13 years**

[24]

41. A report from the Children's Commissioner[25] highlights specific issues for children in care in this regard, including:

- limited access to the internet in children's residential care homes and foster placements;
- lack of support from foster carers and other professionals, and a lack of appropriate safeguarding as a direct result of the responsible adults' lack of digital skills;
- a lack of understanding about the pervasiveness of social media in a young person's life, how safeguarding practices apply to digital activity, and how digital tracking can lead to significant problems for looked after children.

Recommendations

---

[23] Over the internet, under the radar: prevention of online CSE/E in Scotland, Barnardo's, 2017: http://www.barnardos.org.uk/over_the_internet__under_the_radar_report.pdf

[24] Palmer, T (2016) Digital Dangers: the impact of technology on the sexual abuse and exploitation of children and young people, Barnardo's, Barkingside: http://www.barnardos.org.uk/onlineshop/pdf/digital_dangers_report.pdf

[25] (2017) Growing up digital in care. https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/11/Growing-up-Digital-in-Care-CCO.pdf

42. Guidance for children on their data rights and privacy should be published alongside the Code, offering clear advice about what to do and where to go if children are concerned about something online. This guidance should also be promoted to adults responsible for the wellbeing of children, particularly foster carers and professionals working in children's services and residential care homes.

43. The Code should also establish a duty on all online services to signpost independent, specialist advice lines, such as the Professionals Online Safety Helpline, as part of their policies and procedures.

Additional areas in need of a design standard (Q5E)

Age-verification

44. It is widely recognised that online service age-verification systems are ineffective. According to Ofcom, more than half of 12 year olds and 46% of 11 year olds have at least one social media account, despite the minimum age being 13.[26] Given that many of the standards that the Code is likely to set out rely on being able to accurately identify the age of users, and to provide specific, targeted protection to child users, this is a significant problem.

45. The ICO should consider and consult further on what impact a standard on age-verification would have. This should include consideration of mandating age-verification not only for initial access to services (i.e. creating an account), but also for accessing certain content on a platform. The ICO should be mindful of the need to balance the need for robust software while avoiding the risks associated with collecting excessive amounts of sensitive data from children and young people.

Facial recognition/biometrics

46. The growing use of facial recognition software by online services, including the internet of things, has significant and emerging implications for data privacy.

47. While the processing of biometric data is covered by article 9 of GDPR, giving consent to facial recognition features is already integral to the user experience of some services and products (e.g. the iPhone X). This is only likely to increase, with other technology companies such as Facebook rapidly developing their use of facial recognition. The large-scale collection of this data may still be relatively new, but the implications it could have on profiling are already clear. Given this, it is concerning that the prohibition on profiling children is only contained within the recitals of GDPR and therefore does not have the full force of the law (see recitals 71 and 75).

---

[26] Children and Parents media use attitudes 2017, Ofcom: https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

48. Article 9(4) of GDPR leaves the door open for Member States to 'introduce further conditions, including limitations, with regard to the processing of…biometric data', and we believe the Code is a good opportunity for the UK to do that. The ICO should therefore explore the inclusion of standards on facial recognition/biometrics, keeping in mind the need to future-proof the Code as far as is possible.